

North East

ROCU

Regional Organised Crime Unit Network

Monthly Threat Update

North East Economic & Cyber Crime

Welcome to the Monthly Threat Update (MTU) from NEROCU. This document provides an overview of Economic and Cyber crime trends within the North East and UK.

This document contains November 2024 data with a forward outlook.

Please contact the Regional Economic Crime Coordination Centre (RECCC) if you have any questions: RECCC@durham.police.uk

Reading Time 5-10 minutes.

Contents

Looking Back



- [Action Fraud: Regional Cyber Summary](#)
- [Action Fraud: Regional Fraud Summary](#)
- [Engagement Events](#)

Contents

Looking Forward



- [Horizon Scanning](#)
- [What's Happening Next](#)

North East Cyber Crime November Summary



INCREASED THIS MONTH COMPARED TO THE SAME MONTH LAST YEAR

Total Cyber Reports (compared to November 2023)		142 (+39.2%)
Hacking -Social Media and Email		102 (+36%)
Hacking - Personal		17 (+6.3%)
Computer Virus/ Malware		15 (+275%)
Hacking Extortion		8 (+33.3%)

Mobile Account Hacking

There has been an increase in reports of Mobile phone accounts being hacked across the region. One victim has initially reported their email account hacked, and then their mobile phone account. A new Apple iPhone was ordered and a new phone contract was set up in the victim's name. Another victim reported their mobile account being hacked and the suspect ordered a new Samsung phone for £1389, which they set up monthly payments for on the victim's account.

Phishing

Reports of Phishing emails and texts have appeared in all Cyber categories in November's Action Fraud data.

- There has been a continuation of the EVRI text message scam, where the victim submits personal and bank details to rearrange their delivery. This has led to suspects accessing victim's bank accounts.
- There have been TV licensing phishing email scams asking for bank details to renew the licence, providing the suspect with the victim's bank details.
- There have also been reports of phishing emails from Norton Anti-Virus upgrades. One victim reported completing the required information for the upgrade and the suspect gained access to the credit card then applied for a loan and balance transfer.

PayPal

Within the Hacking- Social Media & Email fraud category, there has been a rise in PayPal accounts being hacked. The reports range from the PayPal account being hacked and address details updated and used to order an Xbox. Another victim reported a loss of £1000, which was made to a limited company. A victim from Northumbria reported a £1670 loss, after noticing unrecognised transactions leaving their bank account via PayPal to a Virgin Bet account unknown to them.

North East Fraud November Summary

**DECREASED THIS MONTH
COMPARED TO THE SAME
MONTH LAST YEAR**



Total Fraud Reports (compared to November 2023)	683 (-19.7%)
TOP 5 MOST FRAUD REPORT CATEGORIES THIS MONTH:	
Online Shopping and Auctions	144 (-33.3%)
Advance Fee Frauds	75 (-21.9%)
Other Consumer Fraud	73 (-5.2%)
Cheque, Plastic Card and Online Bank Accounts	49 (-12.5%)
Investment Fraud	44 (-41.3%)

Fake iPhones

There are several reports this month from victims buying iPhones on auction sites or social media marketplaces which turn out to be fake. Counterfeit phones, particularly fake iPhones, have become increasingly prevalent in online markets and more sophisticated and are not immediately identifiable as such.

Impersonation Scam

Fraudsters impersonating banks, phone companies or Amazon continue to target victims in the North East and across the UK. As more safeguarding measures are put in place, fraudsters cold call victims for one-time passwords. There have been an increasing number of reports where the criminal mentions 'Action Fraud' reporting to the victim to add an element of legitimacy to their script.

Online Shopping and Auctions

£135,300 has been lost to victims through Online Shopping and Auctions this month. 36% of Online shopping reports relate to sales through Facebook or Facebook Marketplace and 10% through auction sites Ebay and Gumtree. Items include electronics, furniture, leisure & sports equipment, jewellery, clothes and vehicles. Victims are both buyers and sellers.

Loyalty Points Thefts

This month there has been an increase in Sainsbury's customers reporting that their Nectar card balances have been stolen and used by fraudsters around the UK. This is not a new scam but is re-emerging.

Loyalty points can usually be exchanged for food, clothing, toys, electricals or even flights and have as much value to criminals as they do to their rightful owners. If you find your points are missing, you should contact your loyalty scheme provider immediately using the contact details found on their website.

HAVE A FRAUD FREE CHRISTMAS

Online Shopping and Auction Fraud continues to be the most reported Fraud in the North East.

During the festive season this is expected to rise further as consumer's spending increases over the festive period. Some tips on how to have a Fraud free Christmas are on the next page.

Merry Christmas
from everyone here at the
North East ROCU.

Keywords have been taken from
Online Shopping and Auction Fraud
victim reports to Action Fraud –
October 2024.



Festive Shopping Tips

Check you are using genuine website domain addresses when shopping online.
If you are using Facebook Marketplace, try to see the item in person.
Check reviews of websites before purchasing.

Always use a credit card for large purchases over £100, they offer more protection through section 75 of the consumer credit act.

REMEMBER!!!

If it seems too good to be true, it probably is.

Be wary when looking for deals, especially on social media.

ENGAGEMENT EVENTS

Below is just some of what the team have been up to this month...

The European Money Mule Action campaign (EMMA10) Fraud Roadshow was a huge success and it continued throughout November speaking to hundreds of students across the North East to raise awareness, some of the students that and staff that took part were Durham University, Darlington FE College, University Centre Middlesbrough and Middlesbrough College.

Northumbria Fire Service took part in a Fraud awareness session and Teesside Adult Safeguarding Board took part in CPD with an online session.

This month the team have attended Nissan with partners to speak with staff at the plant about financial wellbeing and general Fraud awareness.

Stockton Council Adult Learning and Northumberland Communities Together both received an input around Fraud awareness.

We hosted a Fraud Awareness day at Natwest Bank in Durham.



EMERGING THREAT

What is happening?

There has been a rise in reports in the Durham area of victims receiving phone calls on withheld numbers impersonating their local police.

During the call, the person impersonating the police states that they have intercepted a payment on the victim's bank card.

The caller then tells the victim to hang up and ring the police, some of the callers have provided false police collar numbers.

How to protect yourself:

- Be aware that once you have hung up, the caller can hold the line for up to 10 minutes. Try to use a different phone or wait a while before making any other phone calls.
- The callers know personal and local information that may make it seem believable, be cautious about giving out personal information.
- If in doubt, hang up!

Find out more:
www.gov.uk/stopthinkfraud

SHOP ONLINE SECURELY THIS FESTIVE SEASON

 ADD TO CART

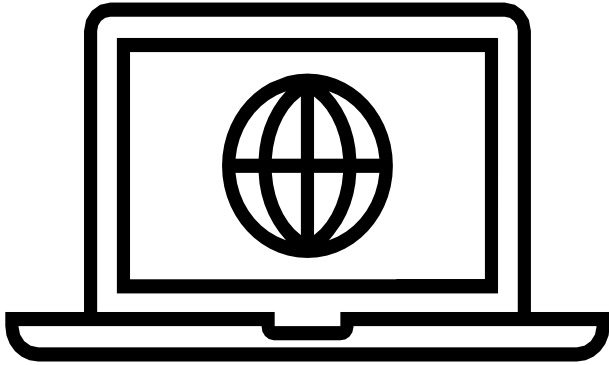


ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

STOP!
THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

Horizon Scanning

Monitoring Threats



We are seeing increased reporting for people purchasing boxed I-phones and discovering it is a fake phone inside the box.

Also, scammers are purchasing legitimate I-phones from sellers and then requesting a refund. When the phone is returned there is no phone in the box.



- If you receive a call out of the blue offering a good deal or refund, do not provide personal or banking information. Contact your network provider on a trusted number.
- If you receive a mobile phone you didn't order, contact the network provider on a trusted number and request any contract is cancelled. Ensure the address you return to is legitimate.
 - Ensure documents with personal information on is shredded before throwing away.
 - Monitor your credit score so you can see any credit searches made under your name.
- When purchasing/selling an I-phone using online marketplaces, be wary and try to see the phone in person before transferring money or issuing a refund.

Rogue Traders

There has been an increase in reports of rogue tradesmen advertising on Facebook, offering fake quotes for work that will not be completed. The deposit is paid by the victim and the 'tradesman' disappears. Sometimes rogue traders also do this by knocking at your door.

If in doubt ... check it out!!!

Do not be rushed into accepting quotes and use online websites such as 'check a trade' or read reviews online where possible.

Advice:

- If you are not expecting anyone, do not answer the door to someone if you are unsure.
- When looking for traders on social media/online, try and find reviews.
- If in any doubt, ask the person to leave or call the Citizens Advice consumer helpline on 0808 223 1133.
 - Don't sign on the spot, shop around.

What's Happening Next?



Looking to escape the cold weather?

After Christmas people will start to look for an escape from the cold weather. Watch out for adverts on social media selling fake holidays and flights.


- Ensure that you are using a legitimate website.
- Make sure your holiday is ABTA or ATOL protected.
- If you are waiting for a refund, ensure you are speaking to the airline or company before sharing any information.

January Sales

As Christmas is approaching people may hope to bag themselves a bargain. Be vigilant when using websites and always check they are secure and the website address is correct before entering any personal or sensitive information. Please follow the advice given in this document to keep yourself safe when making the most of the January sales.





 For more information search 'nerccu police'



Scan to visit our website



BUILDING RESILIENCE AGAINST FRAUD

How to report



Police

All Fraud in the UK is reported to the police at Action Fraud by phone or online:
0300 123 2040
www.actionfraud.police.uk

Action Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Action Fraud.



Emails

Forward Fraudulent emails to
report@phishing.gov.uk



Banks

Dial 159 (Stop Scams UK Anti-Fraud Hotline)
An automated line which Takes you through to your Bank's Fraud team .

For alternative ways of contacting your bank only use the contact details on your bank card or the official website.



Phone Numbers

Forward phone numbers Sending you Fraudulent Messages or calls to **7726**

Handling Instructions

Distribution List
NEROCU
North East Police Forces

Copyright © NEROCU 2024 Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this document, it is provided in good faith on the basis that NEROCU and its staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to NEROCU. Should you or your police force hold information, which corroborates, enhances, or matches or contradicts or casts doubt upon any content published in this document, please contact NEROCU. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

Provenance: Available upon request.



Protective Marking	Official – Law Enforcement
Version	Final
Purpose	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports and open source which have not been verified as true and accurate accounts.
Owner	NEROCU
Authors	Megan Turner – 3P Officer Claire Hardy– Economic Threat Desk Analyst Sarah McCluskey –Cyber Threat Desk Analyst
Reviewed By	T/Sgt Brian Collins

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by NEROCU in confidence and may not be shared other than with the agreed readership/handling code without prior reference to NEROCU. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 2018. The cover sheets must not be detached from the report to which they refer.